CLAIM LISTING

1. (Original) A bitstream for configuring a PLD with an encrypted design comprising:
   a plurality of unencrypted words for controlling loading of configuration data; and
   a plurality of encrypted words specifying the encrypted design.

2. (Original) The bitstream of Claim 1 wherein one of the unencrypted words comprises a key address for locating a decryption key for decrypting the encrypted words.

3. (Original) The bitstream of Claim 1 wherein one of the unencrypted words comprises an address register for loading the first word of the encrypted design.

4. (Original) The bitstream of Claim 1 further comprising a plurality of encrypted words for controlling loading of configuration data, wherein one of the encrypted words for controlling loading of configuration data specifies an address for loading a word of the encrypted design.

5. (Original) The bitstream of Claim 4 wherein another of the encrypted words for controlling loading of configuration data specifies an address for loading a word of the encrypted design.

6. (Original) The bitstream of Claim 1 wherein the unencrypted words for controlling loading of configuration data include a cyclic redundancy checksum for comparison to a cyclic redundancy checksum calculated by the PLD.

7. (Original) The bitstream of Claim 6 wherein the cyclic redundancy checksum in the bitstream is calculated on configuration data before the configuration data has been encrypted.

8. (Original) The bitstream of Claim 6 wherein the cyclic redundancy checksum in the bitstream is calculated on configuration data after the configuration data has been encrypted.

9. (Original) A bitstream for configuring a plurality of PLDs comprising:

a first plurality of words for controlling loading of configuration data into a first PLD; and

a first plurality of words specifying a design for loading into the first PLD

a second plurality of words for controlling loading of configuration data into a second PLD; and

a second plurality of words specifying a design for loading into the second PLD;

wherein at least one of the first and second pluralities of words specifying a design is encrypted.

10. (Original) The bitstream of Claim 9 wherein the first plurality of words specifying a design for loading into the first PLD is unencrypted and the second plurality of words specifying a design for loading into the second PLD is encrypted.

11. (Original) The bitstream of Claim 9 wherein the first plurality of words specifying a design for loading into the first PLD is encrypted and the second plurality of words specifying a design for loading into the second PLD is unencrypted.

12. (Original) The bitstream of Claim 9 wherein both of the first and second pluralities of words specifying a design are encrypted.

13. (Original) The bitstream of Claim 12 wherein the first plurality of words specifying a design for loading into the first PLD are encrypted with a first key and the second plurality of words specifying a design for loading into the second PLD are encrypted with a second key.

14. (Original) The bitstream of Claim 1 wherein the plurality of encrypted words further specify an address into which the encrypted design is to be loaded.

15. (Original) The bitstream of Claim 1 wherein the plurality of unencrypted words for controlling loading of configuration data include a cipher block chaining initial value.

16. (Original) The bitstream of Claim 1 wherein the plurality of encrypted words specifying the encrypted design are loaded into a single group of successive addresses.

17. (Original) The bitstream of Claim 1 wherein the plurality of encrypted words specifying the encrypted design are loaded into a plurality of groups of successive addresses.

18. (Original) A method of generating a bitstream with encrypted design data comprising the steps of:

forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD;

combining the cipher block chaining initial value with a first word of design data to form a first combined word;

encrypting the first combined word to form a first word of encrypted data;

combining the first word of encrypted data with a second word of design data to form a second combined word; and

encrypting the second combined word to form a second word of encrypted data.

19. (Original) The method of Claim 18 wherein subsequent steps of combining and encrypting are repeated until all design data has been encrypted.

20. (Original) The method of Claim 18 wherein the cipher block chaining initial value comprises further bits not part of the starting address for loading a design into a PLD.